SECURE PRINTING TO A WEB-BASED IMAGING PRINT SERVICE

ABSTRACT OF THE DISCLOSURE

Web content is downloaded into a browser from a destination service representing e.g., a printer concurrently with the printer's public encryption key. Image data is encrypted by the web content using conventional public key cryptographic techniques and is then sent to the printer, which contains the private key counterpart of the printer's public key. The encrypted image data is then decrypted using the printer's private key. Since the printer has exclusive control of the private key, secure printing is performed. Each time the browser accesses a different printer, new web content and a new public encryption key are downloaded. The user remains in control of the process, since for each printer accessed the web content and the printer's public encryption key are both downloaded into and operable from the user's browser. In some variations, this capability is applied broadly to web services in addition to printing.